



(19)

Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

EP 1 251 448 A1

(12)

**EUROPEAN PATENT APPLICATION**  
published in accordance with Art. 158(3) EPC

(43) Date of publication:  
23.10.2002 Bulletin 2002/43

(51) Int Cl.7: **G06K 5/00, G06K 19/00,  
G07F 7/10**

(21) Application number: **00976467.1**

(86) International application number:  
**PCT/RU00/00446**

(22) Date of filing: **09.11.2000**

(87) International publication number:  
**WO 01/052174 (19.07.2001 Gazette 2001/29)**

(84) Designated Contracting States:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE TR**

Designated Extension States:  
**AL LT LV MK RO SI**

(30) Priority: 11.01.2000 RU 2000101180

- **GREKOVICH, Alexandre Anatolievich**  
St.Petersburg, 197349 (RU)
- **ROMANOVA, Ljudmila Pavlovna**  
St.Petersburg, 194021 (RU)
- **TATAURSCHIKOV, Sergei Sergeevich**  
St.Petersburg, 194223 (RU)
- **SHTAM, Alexandre Iliich**  
St.Petersburg, 197343 (RU)
- **ZONOV, Viktor Fedorovich**  
Leningradskaya obl., 188660 (RU)

(71) Applicant: **TOO Mnogoprofilnoe Predpriyatiye**  
St.Petersburg, 198092 (RU)

(72) Inventors:  

- **MINKIN, Viktor Albertovich**  
St.Petersburg, 196247 (RU)

(74) Representative: **Viering, Jentschura & Partner**  
**Steinsdorffstrasse 6**  
**80538 München (DE)**

**(54) METHOD, DEVICE AND SYSTEM FOR BIOMETRIC IDENTIFICATION**

(57) For the purpose of user biometric identification, at least one optical image of the selected user biometric parameter (BP), for example, its fingerprint, recorded on a suitable carrier - biometric key (20). The main operations of the identification method is simultaneous or alternating matching of the selected biometric parameter with the inlet optical surface of the readout sensor (57); readout of the specified parameter and its image by the readout sensor with generation of electronic codes of the readout parameter and readout image in the format providing a possibility of their comparison; comparison of the above-mentioned codes and output of the result of identification on the basis of the results of the given comparison. In its preferable version, the method also

provides a stage of for the biometric key manufacture and the formation of database (38) of verified electronic codes of biometric parameters of the users to be subject to identification. User identification system (1) contains a subsystem (10) for the manufacture of biometric keys (20); a subsystem (30) for generation and storage of database (38) of the verified electronic codes of each specified biometric parameter of every user and at least one user identification device (42). This device (42) contains a readout unit (50) containing at least one readout sensor (57) equipped by a multi-element photo-detector (58); a lighter (52); a holder (54) for installation and fixation of any biometric key (20) and a processor unit (60).

**Description**Technical Field

**[0001]** The invention relates to biometric identification with optical reading of biometric information and can be used in any areas where it is needed to carry out user identification including security and access systems, various transactions including financial transaction with the use of personalised credit cards, passport systems for population, manufacture and use of various personalised documents such as driver's licenses, etc. Then to simplify understanding of the invention essence, it will be described mainly with the application to the use as a biometric parameter of one or several fingerprints. However the invention also covers the use of any other biometric parameters being suitable for the identification purposes, for example, retina images or user signatures.

Prior Art

**[0002]** The user identification methods are known that use information not connected with a biometric parameter containing, for example, a personalized identification number (PIN) recorded directly on a plastic card or in the memory of a contact or contact-free chip located on the same plastic card or a special carrier. Information recorded on such card can represent a non-repeatable number or support a ciphered exchange dialogue between the information carried and the reading system (US 6068184, US 5991749). These methods and systems are easy and reliable in operation but are not protected against unauthorised use after loss of the carrier, which can be used by any person.

**[0003]** At the present time, a whole number of user identification systems are known, which use biometric dactyloscopic information. The principle of operation of most similar systems is based on optical reading of a biometric parameter of the user being identified by means of the corresponding reading device, conversion of the readout information into a digital electronic code and search in the database for an electronic code matching, in essence, this electronic code. If such matching takes place, then a signal on a positive result of the user identification will be issued. Similar systems and identification methods implemented therein as well as devices being used in the given systems are described, for example, in US 4933976, US 4932776, US 4785171, US 4690554, US 4582985.

**[0004]** The known systems implementing this principle contain various biometric parameter reading devices differing, in particular, by the type of photo-receiver being used and by the lighter design. So in WO 98/27509, a user identification device is described, which allows to enter a live finger image with a high image quality and which contains a lighter illuminating the user finger and the sensor with the inlet fibre-optic surface, onto which

the user finger is put.

**[0005]** Light scatters in the finger and passes through the skin in places (lines) pressed against the inlet surface, with minimal losses; at places not pressed against the surface (in hollows), the light losses are considerably high. Because of that, an optical image is being created and an electronic fingerprint image based thereon, which is then converted into an electronic code for the image being read out. The lighter design of this device is optimised with the account of light scattering peculiarities in a real ("live") finger, which restricts the use of the given device and the method, which it implements, by the identification by real fingerprint at its comparison with the electronic codes being stored in the database.

**[0006]** Instead of storing user biometric parameter codes in the database, they can be recorded on biometric keys being plastic cards to be issued to users and read out from these keys in order to be compared with a signal being obtained as a result of the corresponding conversion of the read-out biometric parameter, as it has been described, for example, in US 4993068, US 5598474 and US 5623552. The identification signal is issued in case of mutual correspondence of the information written on the card and obtained at the biometric parameter readout.

**[0007]** In particular, a possibility is known to write information, including that on a plastic card, in the form of a two-dimensional bar-code (US 5548110, US 6062481). However recording of dactyloscopic information or a fingerprint code may contain approximately 1 Kbyte, and a two-dimensional bar-code of such size will occupy almost half of the plastic card. Consequently, recording of information about two fingers of the user on one plastic card is practically impossible, since besides dactyloscopic information, PC should provide space for recording the user demographic data. In addition, two-dimensional bar-code readout devices are sufficiently sophisticated and expensive, which also impedes the use of this bar-code for recording of dactyloscopic information on plastic cards in mass projects, in spite of a low cost of the card itself.

**[0008]** A common shortcoming of known identification systems with the use of a contact-free chip plastic card is also a high level of expenses, which is especially sensible at the implementation of such mass personalised projects as issuance of national passports, driver's licenses and other documents. The cost of such projects will be determined mainly by the cost of chip plastic cards. For example, the issue of passports for 100 million people based on a chip plastic card costing approximately USD 15 will require USD 1.5 billion.

**[0009]** The use of contact chip cards for passport project is impossible, as, in spite of a considerably lesser cost (USD.3-5 on average), the reliability of the contact chip operation is not sufficient, as they can easily be subject to destruction.

**[0010]** In connection with the above-listed drawbacks, these devices and systems have not yet reached mass

application.

**[0011]** A system is also known (described in US 4983036), where information written on a plastic card, which is used as a biometric key, is the optic image of a fingerprint. In the identification process, this image is to be compared with the optical image of the real fingerprint by means of autocorrelation of the image of the optically projected fingerprint-reflected light in respect of the fingerprint on the card. A similar comparison method is very laborious and unreliable.

#### Summary of the Invention

**[0012]** The main task, which is the target of this invention, is to ensure a simple, convenient and reliable user biometric identification with the use of at least one optical biometric parameter image being formed on the biometric key.

**[0013]** A further problem is to provide a simple, convenient and reliable user biometric identification with the use of at least one optical biometric parameter image being formed on the biometric key, functioning without the necessity of calling of the verified electronic code database.

**[0014]** The next problem is to secure a simple, convenient and reliable user biometric identification with the joint use of at least one optical biometric parameter image being formed on the biometric key and the information being obtained at the direct reading of the similar biometric parameter by means of an optical readout device or a readout unit.

**[0015]** Another problem is to provide an opportunity to carry out user biometric identification with the use of two protection levels based on verified dactyloscopic information and with the use of one and the same optical readout device or a readout unit for reading of at least one optical image from the biometric key and the similar "real" biometric parameter.

**[0016]** This invention providing the solution of the above listed and other problems, which will be clear from the detailed description of the inventions given herein-after, is based on the experimental establishment of a possibility of reading of optical images of some biometric parameters, first of all, of fingerprints, from the surface of a plastic carrier manufactured from a material with the integral absorption of optical radiation in certain spectrum regions being close to finger absorption. Accordingly, this invention based on the use of optical images of biometric parameters written on a certain plastic carrier (hereinafter referred to as the "biometric key"), represents, in its first aspect, a user identification method including preferably the following operations:

(f) matching of the image of the selected biometric parameter for an individual user, for example, his/her fingerprint, with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected

5 spectral interval; at that the above-mentioned image has been formed on the biometric key of the given user in the area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;

(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image;

(j) matching of the selected biometric parameter with the inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image,

(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and

(n) output of the user identification result based on the results of comparison of electronic codes of the biometric parameter and the readout image.

**[0017]** In one of its preferable implementation options, the method concerning this invention also provides a 30 stage for the biometric key manufacture and the formation of a database of verified electronic codes of biometric parameters of the users to be subject to identification, this stage including the following operations:

(a) selection of the biometric parameter for an individual user, for example, his/her fingerprint;

(b) generation of the optical image of the selected user biometric parameters from a variety of users;

40 (c) recording of the generated image with the scaling being equal or close to 1 on a blank for the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;

(d) generation of at least one verified electronic code of the selected biometric parameter and its saving for permanent storage in the selected format in the form of a set of digital signals unambiguously corresponding to the specified biometric parameter;

50 (e) repeated execution of operations (b), (c) and (d) for the remaining users out of the variety of users with obtaining of one biometric key for each user and with generation of the database of verified electronic codes of selected biometric parameters;

**[0018]** In order to enhance the identification reliability,

the method under this invention can also include additionally the following operations:

- (j) combination of the selected biometric parameter of the user being identified with the above-mentioned inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
- (k) readout of the specified biometric parameter with generation of its electronic code providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;
- (l) search for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter,

with operation (i) additionally including the results of operation (l).

**[0019]** In this implementation version, the identification method at the stage of biometric key manufacture preferably includes the operation of

- (o) generation of all verified electronic code of the selected biometric parameter and its saving for permanent storage for all users out of the variety of users in the form of a set of digital signals unambiguously corresponding to the specified biometric parameter, with generation of the database of verified electronic codes of selected biometric parameters in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;

**[0020]** in addition, operation (m) consists of comparison of the electronic codes of the readout biometric parameter and the readout image with verified electronic codes, and a decision on the positive identification result shall be taken at the detection of a verified electronic code, which, in essence, coincides with the electronic code of the readout biometric parameter and/or readout image.

**[0021]** Examples of materials especially suitable for manufacture of the biometric key are polyvinylchloride (PVC) or polyester (PET), which are conventionally used for the plastic card manufacture. At that, the best results of the readout of optical biometric parameter images are reached at the uniform illumination of the carrier in transmitted light within the selected spectral interval, which preferably lies in the near infrared region (0.75 - 1.0  $\mu\text{m}$ ). In this case, the preferable thickness of the optical image carrier equals to about 0.8 mm, i.e. coincides with the standard thickness of plastic cards. It is evident that the reverse side of the plastic card (opposite to the side, on which the biometric parameter image, for example, fingerprint image, is applied) shall not contain images being non-transparent in the selected region of the spectral interval, as the availability of such

images may lead to the appearance of significant disturbances on the readout biometric parameter image.

**[0022]** The authors of the invention have experimentally established that any colour and grey-scale black-and-white printing of standard printers and DataCard (Image Card Express Photo ID Printer, DataCard 9000) and Fargo (Pro-L, Quatro) plastic card printing systems is transparent in the selected spectral range whereas printing from a black tape is practically non-transparent in the specified spectral range.

**[0023]** The next condition providing a high readout quality is scaling of the biometric parameter image at its generation on the biometric key. There is the only difference in the resolution of readout facilities and means generating the image. For example, normal thermal printing facilities for plastic cards have the resolution not higher than 300 dpi whereas the image readout facilities can have the resolution up to 3000 dpi. Analysing large dactyloscopic image archives, the authors have established that the number of visible dactyloscopic peculiarities suitable for identification increases as the resolution of a dactyloscopic scanner grows. As a consequence of this dependence, it appears that, for example, at printing of a fingerprint image or its part enlarged proportionally to the reduction in the area with constant resolution, an approximately equal number of critical points both on the whole fingerprint and on its part. Consequently, the location of the enlarged image of the central part of the fingerprint on the plastic card is an additional measure allowing to avoid errors during the identification, as at every placing of the user finger, the probability of presence of the central fingerprint part is considerably higher than that of its edge parts.

**[0024]** At least two images of the corresponding biometric parameters can be generated on one biometric key preferably made in the form of a plastic card. An opportunity to place several fingerprint images on one plastic card significantly increases the probability of proper identification; the central-symmetrical location of fingerprints on the plastic card allows not to use moving mechanical parts in the readout unit of the identification device.

**[0025]** According to the second aspect of this invention, in order to execute all above-listed operations of the proposed method, it is provided to create a user identification system containing the following:

- 50 a means for recording of at least one image of one biometric parameter of an individual user out of the variety of users, for example, his/her fingerprints, on a biometric key blank, in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;
- 55 a subsystem for generation and storage of the database of verified electronic codes for each speci-

fied biometric parameter of every user out of the variety of users; and at least one user identification device.

**[0026]** In accordance with the next aspect of this invention, it is also provided to create a new user identification device, which contains the following:

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of user out of the variety of users and contains an image area made from a material being semi-transparent in the selected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the selected scaling;

a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical range;

a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and by means for comparison of the electronic code of the readout image with other electronic codes with generation of the first signal in case of detection of coincidence of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

**[0027]** Besides those mentioned above, one more preferable condition providing high quality readout is the use of a readout sensor with the inlet fibre-optic surface, against which the image being read out must be tightly pressed. At the performance of this and other conditions listed, a possibility of using similar or even one and the same optical readout sensor for reading a real biometric parameter (a fingerprint, i.e. a relief object) and its flat carrier from the plastic carrier.

**[0028]** The use of one sensor for reading both a live finger image and a visible image from the card allows to simplify the identification device design and operations to be executed by the user at the implementation of the identification method under this invention. In addition, the system operation reliability gets considerably enhanced, as unlike a chip PC a fingerprint being stored in the form of a real visible image on the biometric key made in the form of a plastic card has a good noise immunity and does not sensitive to electric and magnetic

fields. Another advantage of this device is an additional possibility of future modernisation and the compatibility meaning that the software identification algorithms are being constantly improved, with the main modifications

5 concerning conversion of the image into a compressed code. In a chip, only a compressed code is stored, which will not allow or impede a future use of any new software. The information storage in the form of an optical image of the biometric parameter will allow to use all future software improvements without any considerable expenses, this being simultaneously for reading of both the biometric parameter itself and its image on the biometric key.

**[0029]** The above-listed advantages make it impossible to broadly use the proposed invention, both for local systems and for global projects, for example, national passport system, authorisation of access to Internet or additional protection of credit cards.

**[0030]** The remaining distinctive signs and advantages of this invention will become clear from the detailed description of preferable versions of its implementation given below as well as from the invention formula being enclosed herewith.

**25** Brief description of drawings

**[0031]**

**30** Fig. 1 shows one of the preferable versions of embodiment of the user identification system under this invention in the form of a flow-chart;

Fig. 2 shows the front side of a plastic card;

Fig. 3A contains a user identification device in the form of an arrangement with the biometric key being introduced therein;

Fig. 3B shows the same device with a user finger being placed into it;

Fig. 4 shows a set of operations to be executed at the first stage of one of the preferable versions of implementation of the method under this invention; Fig. 5A, 5B show a non-processed image and a processed image of one and the same fingerprint respectively;

Fig. 6, 7 and 8 show sets of operations to be executed at the second stage of two preferable versions of implementation of the method under this invention.

**50** Description of preferable implementation of the invention

**[0032]** The system version shown in Fig. 1 and designated on the whole as 1 is intended mainly for operation with biometric keys in the form of plastic cards with 55 the standard parameters in accordance with ISO 7810-85 and sizes in accordance with CR80. However it can also be used for manufacture and use of many other versions of biometric keys. As shown in Fig. 1, sys-

tem 1 consists of several interconnected parts, or subsystems, the main from which are subsystem 10 for manufacture of biometric keys 20, subsystem 30 for generation and storage of the verified electronic code database and subsystem 40 for identification.

**[0033]** Subsystem 10 for the manufacture of biometric keys includes a set of necessary technical means or devices to execute various operations provided by the key manufacture technology being used in the system. It is evident that the composition of this set and the form of embodiment of its components considerably depend upon a specific version of the identification key being used. However an obligatory part of any version of system 10 are means for recording the optical image of the selected biometric parameter on biometric key 20. These means of recording preferably include device 12 for generation of an image of the selected biometric parameter with the conversion of this image into its electronic copy, i.e. into a set of electrical (or other) signals unambiguously corresponding to the image being generated. Device 12 can operate in any wavelength range and/or use any suitable image generation and conversion means provided the quality of the electronic copy being obtained is sufficient for the subsequent creation of an optical image on the biometric key being suitable for the performance of the user identification function. As device 12, for example, any scanner or a device for reading biometric parameters, for example, a dactyloscopic scanner, can be used for obtaining of a fingerprint image and/or a television camera for obtaining of user retina or face images.

**[0034]** Another, not obligatory but preferable, component of subsystem 10 is device 14 for electronic copy processing. The type of processing being performed by this device will be explained later at the description of the identification method under this invention. A preferable version of implementation of device 14 is a personal computer equipped by the corresponding software program for processing images and by necessary peripheral devices, including keyboard 15, display 16 as well as an interface (not shown) for reading electronic copies being supplied from the outlet of device 12 for image generation.

**[0035]** The third component of the means of recording is device 18 for application of an optical image on biometric keys 20. Preferably, device 18 is a printer for personalisation of plastic cards connected to the outlet of device 14 and customised for printing images in case of obtaining of processed or non-processed electronic copy from device 14.

**[0036]** Fig. 2 shows a conventional image of the front side of the biometric key pattern in the form of a personalised plastic card with standard parameters in accordance with ISO 7810-85 and sizes in accordance with CR80 (85 mm x 54 mm x 0.8 mm). As shown in Fig. 2, two areas 22 of image are provided for printing the image on biometric key 20, which are made from a material being semi-transparent in the selected spectral interval

of the optical range (for example, 0.75 - 1.0  $\mu$ m, i.e. in the near IR-region). If the biometric key is a plastic card, then the whole card can be made from this material. In particular, suitable materials for area 22 and the biometric key on the whole are polyvinylchloride and polyester.

**[0037]** It can be seen from Fig. 2 that biometric key 20 may, beside a biometric parameter image or several similar images (for example, fingerprints of two or more different fingers of the user), also contain any other necessary information in the wording, digital, symbolic, graphical. Electronic, magnetic or any other suitable form.

**[0038]** An additional information can be written on the biometric key at the same time with recording of the biometric parameter image, with the use of one and the same device 18 for the application of images, or at any other suitable stage of the biometric key manufacture, with the use of any means being suitable for this purpose. As these means are well-known to specialists, there is no need of describing them. The use of thin transparent laminating coatings allows to increase the plastic card service life and does not impede the reading of biometric images from a plastic cards in the reflected and transmitted light. A card can be created with an increased protection and secrecy, as it has been described, for example, in US 4999065. However the availability of an image of the user biometric parameter directly on a plastic card provides its protection better than any other complicated systems, as it makes it practically

impossible to use cards by any other person rather than the user. Coded information can be additionally recorded into biometric key 20, for example, in the form of an n-dimensional bar-code, with the coded information recorded area being selected close to the image size. The coded information may contain, for example, data on the user biometric parameter. In this case, the optical image and the coded information will preferably be recorded by means of various printing means, for example, various paints being non-transparent and/or reflecting radiation in various spectral intervals of the optical range. It is also desirable that the image and the coded information should be placed in a single readout area, which dimensions are determined by dimensions of the photo-sensitive surface of the readout sensor but are separated spatially. In this case, the image is preferably located in the centre of the readout area and the coded information is located in the edge zone of this area.

**[0039]** The main component of subsystem 30 for generation and storage of the verified electronic code database is processor 32 equipped by the corresponding peripheral devices 34 and connected with the outlet of processing device 14 for the reception of processed electronic copies of optical images being generated by this device. In the preferable version of implementation, subsystem 30 is a personal computer. As it will be described in detail later, this subsystem is designed for the conversion of electronic copies coming from device 14 into verified electronic codes of the corresponding user

biometric parameter (or biometric parameters) as well as for generation and storage of database 38 of such codes. In the alternative version of implementation of subsystems 10 and 30 (not shown), processing device 14 is a part of subsystem 30, which one outlet in this case shall be connected with device 18 for application of optical image on biometric key 20. It is possible to implement subsystem 30 and device 14 for the electronic copy processing on one personal computer.

**[0040]** Identification subsystem 40 in its preferable version is an identification device 42 connected to database 44 of subsystem 30 data with a possibility of data exchange. One of the preferable versions of implementation of device 42 is given in Fig. 3. In this version, device 42 contains a readout unit 50 and a processor unit 60 connected to the readout unit outlet. Readout unit 50 in the given version consists of a lighter 52, a holder 54 of biometric key 20 in the form of a plastic card and a readout sensor 57 with a multi-element photo-detector 58 (matrix or linear) being sensitive in the selected spectral interval of the optical range.

**[0041]** At the use of the biometric key in the form of a plastic card and at the selected spectral interval in the near IR-region, the preferable version of photo-detector 58 is a matrix detector with the size of photo-detecting surface being not less than 8 x 12 mm, with the number of photo-detecting elements being not less than 200 x 300, with a fibre-optic washer 59 generating the inlet surface of sensor 57. A specific version of the sensor can be the DactoChip DC-21 model with the size of photo-detecting surface being equal to 10 (H) x 15 (V) mm and with the number of photo-detecting elements of 512 (H) x 576 (V), with the fibre-optic washer of the brand **ИАШО** 200370002 TY with the diameter of one optical fibre being equal to 6  $\mu\text{m}$ . At the use of photo-detector 58 in the form of a ruler, the device can be equipped by a scanning mechanism providing reciprocal photo-detector movement in the plane being parallel to the plane of fibre-optical washer 59. Alternatively, scanning can be carried out by moving the biometric parameter in respect to the ruler of photo-detector 58.

**[0042]** Lighter 52 is preferably made of the impulse type and contains not less than one light-emitting diode (LED), for example two LEDs of the brand **ИПС-1-800/90** emitting light in the selected spectral interval ( $\lambda = 800 \text{ nm}$ ,  $\angle = 90^\circ$ ).

**[0043]** It was assumed earlier that in order to obtain a uniform fingerprint image in the light transmitting through the finger, it shall be illuminated non-uniformly directing more light into the volumetric part of the figure, as it is known that the light scattering in any medium, including finger, is proportional to the light transmission path.

**[0044]** The authors of the invention have experimentally proved that such diffuse scattering really occurs at the local illumination of the finger by a narrow-directed light, however this fact with application to this invention is not significant, as the narrow-directed illumination is

unsuitable for raying of thin (as compared with a finger) plastic cards, as it creates a high light non-uniformity. At the same time, the authors have experimentally established that at the initial uniform diffuse illumination of the sensor surface, the same uniform illumination (raying) occurs for both the plastic card and the finger at the use of a lighter operating in the near IR-region of the spectrum.

**[0045]** Holder 54 shall tightly press the plastic card against the inlet surface 59 of sensor 57 and at the same time not admit any surface damage of plastic card 20 at its mechanical movement between the surfaces of holder 54 and sensor 57. In order to meet this requirement, holder 54 is preferably made from a metal (for example, aluminium), on which internal (contacting with the plastic card) side 55 a layer 56 of a fluffy material (optical suede) is glued. Such design provide an easy and high-precision placing of the plastic card over sensor 57 without the use of moving mechanical parts in the design of readout unit 50.

**[0046]** A distinctive peculiarity of the readout unit 50 in the given version of the device is the fact that is provided a possibility of bringing into contact with the inlet surface 59 of sensor 57 of not only the biometric key 20 but also directly any finger of the user being identified, as it is schematically shown in Fig. 3B. So holder 54 combines two functions: it fixes both the plastic card, and the user finger. To this end, holder 54 in the centre has a hollow enabling the user to fix a finger conveniently on the inlet surface of the sensor. Normally the finger holder is installed tightly pressed against the dactyloscopic sensor (sensor 57). However the fixation of the bottom plane of the holder, proposed by the authors and shown in Fig. 3, at the height of the plastic card in respect of the inlet surface of the sensor also allows to provide a good contact between the user finger and the inlet surface of the sensor. It is evident that in the given holder the illumination of the finger being placed into it is provided from the side being opposite to the area of contact between the finger and photo-detector 58 and can be carried out from the top or from the sides.

**[0047]** Processor unit 60 is preferably made on the basis of a suitable personal computer of the PII-400 level with the corresponding peripheral devices (not shown). This computer is connected to the outlet of the readout unit 50, for example, by means of the corresponding cable connected to the parallel port of the computer. The processor unit 60 shall be equipped by means for generation of the electronic code of the readout image and the readout biometric parameter as well as by means for comparison of the electronic code of the readout image with the electronic code of the readout biometric parameter or verified electronic codes. These means are preferably software programs, for example, made on the basis of a standard dactyloscopic identification program; however any of them can also be implemented in the form of a separate specialised electronic module being a part of a computer or made sep-

arately from it.

**[0048]** In the case when coded data are additionally applied on the biometric key, for example in the form of an n-dimensional bar-code, readout unit 50 and processor unit 60 shall be made with a possibility of reading of the specified data and its decoding respectively. Meeting if this condition is facilitated at placing of the readout image and the coded information in a single readout area, due to which a single readout sensor 57 can read out both the image and the coded information.

**[0049]** Then the main stages of the identification method under this invention will be described.

**[0050]** The first stage 100, when the manufacture of biometric keys and preferably databases takes place, is performed with the use of subsystems 10 and 30 shown in Fig. 1. As shown in Fig. 4, the implementation of this stage begins from operation 102 for the biometric parameter selection of a biometric parameter (or parameters) for system 1. The second operation 104 consists of the input of the selected user biometric parameter included into the variety of users by system 1, in the field of vision of the image generation device 12 of subsystem 10. With application to the considered version of the method under this invention, the selected biometric parameter is a print of a certain user finger.

**[0051]** The next operation 106 for generation of the optical image of the selected biometric parameter of the given user, i.e. obtaining of optical information unambiguously corresponding to the given biometric parameter, is carried out with the use of the corresponding device 12 of subsystem 10 (see Fig. 1), for example, a readout unit (similar to unit 50 shown in Fig. 3b), which also performs the subsequent operation 108 for conversion of the optical information into electric information, with obtaining of an electronic copy of the biometric parameter, i.e. the corresponding set of electric signals unambiguously matching the specific biometric parameter.

**[0052]** The next operation 110 is coding, i.e. conversion of the electronic copy into the digital code of the selected biometric parameter. As it is shown in Fig. 1, this operation is executed in device 14 for electronic copy processing connected to the outlet of device 12.

**[0053]** It is expedient to use device 14 also for execution of operation 112 - electronic copy processing with isolation of information from it necessary and sufficient for the biometric parameter identification. This operation preferably includes binarisation of the electronic analogue of the grey-scale fingerprint being generated by device 12 (see Fig. 5A) with obtaining of the processed analogue, so-called "skeleton" (see Fig. 5B) of a fingerprint with constant line thickness reflecting only those image features, which are taken into account at identification. The image processing monitoring can be carried out, for example, by means of a display 16 being a part of subsystem 10. The electronic copy of the selected biometric parameter being processed is fed to a printer or any other suitable device 18 for application of an optical image in order to execute operation 114 for re-

cording of the processed optical image at the biometric key blank, with obtaining of biometric key 20. As it has been mentioned, this record is made in the image area made from a material (for example, polyvinylchloride)

5 being semi-transparent in the selected spectral interval of the optical range. The recording is performed with the scaling being equal or close to 1, i.e. the processed fingerprint image being recorded (see Fig. 5B) by its dimensions equal or close to the real fingerprint, and, 10 more precisely, to those parameters, which are taken into account at identification, namely: reflects the papillary line pattern. In order to carry out the recording, paints or other printing means are used, which are non-transparent or reflect radiation in the specified spectral 15 interval, for example, a black tape of the Pro-L printer manufactured by Fargo.

**[0054]** Operation 114 for the processed image recording can also provide recording of any user data or any other necessary information on a blank of the biometric 20 key 20, for example, that given in Fig. 2. This information can be entered into subsystem 10 by means of peripheral devices, for example, keyboard 15 or any external systems not shown in Fig. 1. In the alternative version, any other information (which application on the biometric key is not obligatory for the implementation of the 25 method being described) can be recorded on the biometric key both before and after execution of operation 114.

**[0055]** After that, with the use of subsystem 40, procedure 201 is performed for the user identification according to the biometric key 20 and the selected fingerprint (performance of the given identification version will be described later, with reference to Fig. 6). In case of an identification failure, the key is rejected and the operations described shall be repeated in order to manufacture a valid key.

**[0056]** In case of confirmation of identification, the biometric key is recognised valid and can be issued to the user (operation 116). In this case, the digital information 40 being used for recording of the optical image on the biometric key will also enter into subsystem 30 for generation and storage of the verified electronic code database. Here in processor 32, its processing will be completed, i.e. operation 118 for generation of the verified 45 (i.e. unambiguously matching) electronic code of the selected biometric parameter, which enters for storage into database 38 (operation 120).

**[0057]** All operations described above are performed for all persons included into the variety of users by the 50 identification system under this invention.

**[0058]** For the simplicity of understanding, the first stage of implementation of the given method was described in the simplest version. It is evident that in case of identification by several biometric parameters, operations 102-120 shall be repeated for each of the parameters. In order to enhance system operation reliability, several optical images can be generated for each selected biometric parameter at the execution of operation

106, out of which, upon results of the reference identification, the final selection of one image being the best or generalised to be applied on the biometric key shall be carried out. In this case, verified electronic codes of all generated optical images of one biometric parameter can be formed and entered into database 38.

[0059] The enhancement of the identification system reliability can also be reached by the manufacture of all or at least a part of biometric keys in several copies.

[0060] The with the reference to Fig. 1, 3 and 6, one of the preferable versions of implementation of the second stage of the proposed method will be considered, namely, the conduction of user identification by biometric key. In order to implement this version, it required to provide a possibility of access from means 68 for electronic code comparison of the processor unit 60 of the identification device 42 to database 38 of system 1, as shown in Fig. 1. Alternatively, the whole database 38 or its corresponding fragment can be transferred into the identification device 40, which in that case can operate fully independently. This version can be expedient, for example, in cases when the manufacture and use of biometric keys is carried out in different organisations or if a variety of independently functioning identification devices is used installed at a considerable distance from the place of location of subsystem 30 for generation and storage of the verified electronic code database.

[0061] It can be seen from Fig. 6 that in this version the identification stage 201 includes procedure 210 for obtaining of an electronic code of the image. For its execution, the user shall enter his/her biometric key into holder 54 of the readout unit 50 of the identification device 42, i.e. perform operation 212 of matching of the biometric parameter image on the biometric key 20 with the inlet optical surface of the readout sensor 57. The readout unit consecutively executes operations 214, 216 for reading out of the specified image and generation of an electronic code of the image. At the execution of operation 216, the same electronic code format is used as at generation of the verified electronic codes (during operation 118) or any other format permitting a possibility of comparison of the electronic code of the image with the verified electronic codes. Procedure 210 is terminated by operation 218 for recording of the electronic code of the image.

[0062] Then operation 230 for the search in database of a verified electronic code, which, in essence (i.e. with the accuracy up to the established matching threshold), coincides with the electronic code of the readout image. The reliability of such search is very high, in the first place, because the image recorded on the biometric key is optimised for the search purposes by means of exclusion of all excessive and interfering information (as it was described earlier) and, in the second place, due to the fact that the key manufacture technology provides a high image stability in time, i.e. it is not subject to temporal changes being typical, for example, for real fingerprints (in particular, in connection with possible damage

and/or contamination). In addition, holder 54 of device 42 provides very thin and stable combination of the biometric parameter image on the biometric key with the inlet surface of the readout sensor 57. Practice shows

5 that one cannot reach similar stability in respect of user fingers, as at least a part of users are characterised by a low reproducibility of placing a finger on the readout sensor. On average, from 10% to 20% users have difficulties with dactyloscopic identification whereas the error level in case of application of the barometric key under this invention is significantly lower.

[0063] If as a result of search has been found, at least one verified electronic code matching the readout image code, device 42 will generate the corresponding (visual, 15 audio and/or any other) signal on the identification taken place (operation 260). Otherwise a signal on the negative identification result will be issued. In parallel, the corresponding signal can also be given to any executive mechanism (mechanisms), for example, to a mechanism of automatic opening of a door into a room with controlled access.

[0064] It is evident that in case of the use of a biometric key with images of several parameters, all above-described operations of this stage will be repeated for 25 all these images. At that, the symmetrical location of the biometric parameter images on the biometric key in respect of its centre allows to sufficiently simply provide the consecutive matching of specified images with the inlet optical surface of the readout sensor 54 by means 30 of turning of the biometric key 20 around the axis passing through its centre perpendicular to the key plane.

[0065] Though the identification version being described provides, with high reliability, the confirmation of 35 authenticity of the image presented in order to identify the user, it in essence does not identify the user itself but only the biometric key, which it represents, i.e. does not prevent a danger of presentation of the key not by the person, to whom this key was issued.

[0066] The alternative versions of the proposed 40 method are free from this limitations, according to which both the selected biometric parameter and the biometric key are jointly used for the identification purposes. First an identification version will be considered, which can be implemented without calling the database.

[0067] In the given version, the identification stage 45 201 provides the execution, in any order, of the above-mentioned procedure 210 for obtaining of the electronic code of the readout image and procedure 220 for obtaining of the electronic code of the n\biometric parameter (see Fig. 7).

[0068] Procedure 220 consists of operations 222-228 similar to the described operation 212-218 but being executed at placing of a user finger carrying the selected biometric parameter into the readout unit 50. In order to 55 provide the compatibility of the given version of implementation of the method with other alternative versions, it is expedient to use the same electronic code format at the execution of operations 216, 226 as at generation

of the verified electronic codes (during operation 118) or any other format permitting a possibility of comparison of electronic codes of the readout image and the readout biometric parameter with the verified electronic codes.

**[0069]** Upon termination of procedures 210 and 220, processor unit 60 of the identification device 42 performs operation 240 for comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image. Upon results of this comparison, device 42 generates the corresponding (visual, audio and/or any other) signal on the identification taken place or on the identification failure.

**[0070]** Fig. 8 shows another version of implementation of the identification stage 202 providing the attraction of both the biometric parameter and its image with calling the database. This version, like version 201 shown in Fig. 6 and 7, includes procedures 210 and 220 for obtaining of electronic codes in combination of the described operation 240 for the comparison of these electronic codes and with the additional operation 250 for the search in the database for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter and/or readout image. In case of application of the given version, the increase of probability of the accurate identification can be reached not only by the conduction of identification by several biometric parameters and/or several images of these parameters but also with the use of several verified electronic codes corresponding to each or several biometric parameters out of the selected ones. It allows to make the identification probability being close to 100% and, accordingly, reduce the error probability practically to zero.

**[0071]** One should also note that the described versions of identification with the use of the optical image of the biometric parameter can be used in combination with other suitable identification methods, for example, by voice, secret personal identification number (PIN), password, etc. In particular, a high identification effectiveness with the use of this invention has been proved by its experimental verification conducted on a group of users being employees of the applicant-company of this invention with the use of biometric keys in the form of plastic cards carrying processed optical images of two fingers with symmetrical location of images in respect of the central point of the map. These keys have been used in combination with "live" fingerprints and personal numbers of the users being entered by them on the keyboard of the identification device 42.

**[0072]** For specialists in the given area, numerous modifications, which can be introduced into this invention without coming out beyond its limits, will be evident. For example, instead of fingerprints, any other biometric parameters can be used, which allow to generate and record their optical images. The biometric key body (except the image area) can be made from any strong and safe material; any shape providing a possibility of a tight

contact of the image area or areas with the inlet surface of the readout sensor can be given to the keys. Though the described design of the sensor being capable to read out information directly from a finger or a biometric

5 key seems to be preferable; for several versions of implementation of the invention, sensors designed for the operation only with biometric keys of various shape are also suitable.

**[0073]** The functions of the device for electronic copy 10 processing in the subsystem for the manufacture of biometric keys, the subsystem for generation and storage of the verified electronic code database and the processor unit of the identification device can be made on the basis of a single central computer connected with wired 15 or wireless communication lines with a device for generation of the image of the selected biometric parameter, with the device for recording of the image and with all identification subsystems. One or two readout sensors and one or two holders, one of which is optimised for 20 installation of the biometric key into it, and the second one - for placing of the user finger, can be provided in the identification device.

**[0074]** The readout device being described can also 25 be used as an image generation device. In addition, the readout device can be equipped by means providing a possibility to surely distinguish electronic codes being obtained from a real biometric parameter and from its optical image on the biometric key, for example, by the availability of the pulse (see US 3639905; WO 98/27509) or other physiological characteristics (as it is 30 described in US 5719950). The availability of such means considerable reduces the probability of forgeries, i.e. contributes to further enhancement of the identification reliability.

35

## Claims

1. User identification method providing a stage for biometric key manufacture and database generation and a stage for the conduction of identification, with the stage for biometric key manufacture and database generation including the following operations:
- 40 (a) selection of the biometric parameter of an individual user, for example, a fingerprint;
- (b) generation of the optical image of the selected user biometric parameter out of the variety of users;
- 45 (c) recording of the generated image with the selected scaling on a blank of the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in the specified spectral interval;
- 50 (d) generation and saving for permanent stor-
- 55

age in the selected format, of at least one verified electronic code of the selected biometric parameter in the form of a set of digital signals unambiguously matching the specified biometric parameter;

(e) repetition of operations (b), (c) and (d) for remaining users out of the variety of users with obtaining one biometric key each for every user and with generation of the database of verified electronic codes of the selected biometric parameters;

with the identification stage including the following operations:

(f) matching of the image on the biometric key of any user being identified out of the variety of users with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image in the format providing a possibility of comparison of the electronic code of the image with the verified electronic codes;

(h) search for a verified electronic code coinciding, in essence, with the electronic code of the readout image, and

(i) output of the user identification result on the basis of the search results.

2. Method as per claim 1, **characterized in that** it additionally includes the following operations:

(j) matching of the selected biometric parameter of the user being identified with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;

(l) search for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter,

with the operation (i) additionally including the account of results of the operation (l).

3. User identification method providing a stage for biometric key manufacture and a stage for the conduction of identification, with the stage for biometric key manufacture including the following operations:

(a) selection of at least one biometric parameter

5

of an individual user, for example, his/her fingerprint;

(b) generation of the image of the selected user biometric parameter out of the variety of users;

(c) recording of the generated image with the being equal or close to 1, on a blank of the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in the specified spectral interval,

(e) repetition of operations (b), (c) for remaining users out of the variety of users with obtaining one biometric key each for every user;

with the identification stage including the following operations:

(f) matching of the image on the biometric key of any user being identified out of the variety of users with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image;

(j) matching of the selected biometric parameter with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(k) readout of the above-mentioned biometric parameter of the user being identified with generation of his/her electronic code in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image;

(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and

(n) output of the user identification result based on the comparison of electronic codes of the readout biometric parameter and the readout image.

45

4. Method as per claim 3, **characterized in that** for each user out of at least a part of the specified variety of users, at least two biometric parameters are being selected;

operations (b), (e), (f), (g) shall be performed for all images to be recorded on the specified user biometric key;

operations (j) and (k) shall be performed for all biometric parameters of the same user;

operation (m) shall be performed for electronic codes of all readout biometric parameters and all readout images;

operation (n) shall be performed on the basis

50

55

of the results of comparison of electronic codes of each readout biometric parameter and each readout image.

5. Method as per claim 3 or 4, **characterized in that** the biometric key manufacture stage additionally includes the operation:

(o) generating and saving for permanent storage of verified electronic codes for all selected biometric parameters of all users out of the variety of users in the form of a set of digital signals unambiguously matching the specified biometric parameters, with generation of the database of verified electronic codes of selected biometric parameters in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;

10 in addition, operation (n) consists of the comparison of the electronic codes of the readout biometric parameter and the readout image with the verified electronic codes, and the decision on the positive identification result shall be taken at the detection of a verified electronic code, which, in essence, coincides with the electronic code of the readout biometric parameter and/or readout image.

15

20 8. Method as per claim 7, **characterized in that** each biometric key out of at least a part of the specified variety of biometric keys contains images of at least two selected biometric parameters on one user located central-symmetrically on the biometric key;

25 operations (f) and (g) shall be performed for all images contained on the specified biometric key;

operations (j) and (k) shall be performed for all selected biometric parameters of the same user;

30 operation (m) shall be performed for electronic codes of all readout biometric parameters and all readout images;

35 operation (n) shall be performed on the basis of the results of comparison of electronic codes of all readout biometric parameters and all readout images.

30 9. Method as per any of the previous claims, wherein the specified image is a binary black-and-white image.

40

45 10. Method as per any of the previous claims, wherein the fingerprint is selected as a biometric parameter.

50 11. Method as per claim 10, **characterized in that** the operation (b) for generation of the image additionally includes image processing providing the enhancement of reliability of results at the execution of operation (g) for comparison of the electronic code of the readout image with the verified electronic images.

55

12. Method as per claim 1, **characterized in that** the image processing includes generation of a fingerprint skeleton with constant line thickness not less than doubling the resolution of the readout sensor.

13. Method as per any of the previous claims, wherein

(j) matching of the selected biometric parameter with the inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image,

(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and

(n) output of the user identification result based on the results of comparison of electronic codes of the biometric parameter and the readout image.

a plastic card is selected as a biometric key.

14. Method as per any of the previous claims, wherein at the readout of specified image the image area is illuminated from the side reverse in respect of the side, on which the specified image has been generated.

15. Method as per any of the previous claims, wherein a coded information is additionally recorded on the biometric key, for example, in the form of n-dimensional bar-code, with the dimensions of the coded information recording area being selected close to the image dimensions.

16. Method as per any of claims 2-6, wherein the operations (b), (f), (g), (j) and (k) are performed with the use of one readout sensor.

17. User identification device comprising

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of user out of the variety of users and contains an image area made from a material being semi-transparent in the selected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the selected scaling;

a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical range;

a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and

a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and by means for comparison of the electronic code of the readout image with other electronic codes with generation of the first signal in case of detection of coincidence of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

18. Identification device as per claim 17, wherein the specified image is a binary black-and-white image.

19. Identification device as per claim 17 or 18, wherein the scaling factor equals or close to 1.

20. Identification device as per any of claims 17-19, wherein the specified inlet optical surface of the readout sensor is made of optical fibre.

21. Identification device as per any of claims 17-20, wherein a fingerprint is the specified biometric parameter.

22. Identification device as per claim 21, wherein the specified image is a fingerprint skeleton with the constant line thickness not less than doubling the resolution of the readout sensor.

23. Identification device as per any of claims 17-22, wherein a plastic card is selected as the biometric key.

24. Identification device as per any of claims 17-23, wherein the lighter is made capable to illuminate the biometric key being installed into the holder from the side being reverse in respect of the side, on which the specified image has been generated.

25. Identification device as per any of claims 17-26, wherein a coded information, for example, in the form of an n-dimensional bar-code is additionally recorded on the specified biometric key; in addition, the readout unit and the processor unit are made with a possibility of reading of the specified coded information and its decoding respectively.

26. Identification device as per claim 25, wherein the coded information contains data on the user biometric parameter.

27. Identification device as per claim 25 or 26, wherein the image and the coded information are located on the biometric key in a single readout area, which dimensions are determined by the dimensions of the photo-detecting surface of the readout sensor but are separated spatially.

28. Identification device as per any of claims 25-27, wherein the image is located in the centre of the readout region and the coded information is located in the edge area of the readout region.

29. Identification device as per any of claims 17-28, wherein each of at least a part of specified variety of biometric keys contains images of at least two selected biometric parameters of one user located symmetrically in respect of the centre of specified biometric key; in addition, the device is made with a possibility of consecutive matching of all specified images with the inlet optical surface of the readout sensor by means of turning of the biometric key around the axis passing through its centre perpendicular to the key plane.

30. Identification device as per claim 29, wherein the specified images and/or the coded information are recorded by means of various printing facilities, for example, various paints being non-transparent and/or reflecting radiation in various spectral interval of the optical range.

5

31. Identification device as per any of claims 17-30, wherein the holder is made with an additional possibility of assurance of a contact between the biometric parameter and the specified inlet surface of the readout sensor, and the readout unit is made with an additional possibility of reading of the specified user biometric parameter.

10

15

32. Identification device as per claim 31, wherein the processor unit is made with a possibility of storage or reception of verified electronic codes of the selected biometric parameter in the form of a set of a set of digital signals, each of which unambiguously corresponds to the specified biometric parameter of one of the users out of variety of users, and the means for comparison of the given unit are made with a possibility of conduction of the comparison of the electronic codes of the readout image and the readout biometric parameter with the specified verified electronic codes.

20

25

33. User identification system containing the following:

means for recording at least of the optical image of one biometric parameter of an individual user out of the variety of users, for example, his/her fingerprint, on a blank of the biometric key in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;

30

a subsystem for generation and storage of the database of verified electronic codes for each specified biometric parameter of every user out of the variety of users; and at least one user identification device containing the following:

35

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of one user out of a group of users and contains the image area made from a material being semi-transparent in the se-

40

45

50

55

lected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the scaling equal or close to 1, a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical range, a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and the readout biometric parameter and by means for comparison of the electronic code of the readout image and/or the electronic code of the readout biometric parameter, with generation of the first signal in case of detection of coincidence, in essence, of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

34. Identification system containing the following:

means for recording, with the scaling equal or close to 1, of least of the optical image of the biometric parameter of an individual user out of the variety of users, for example, his/her fingerprint, on a blank of the biometric key in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval,

at least one user identification device made in accordance with any of items 19-31.

35. Identification system as per claim 34, wherein it additionally contains a subsystem for generation and storage of the database of verified electronic codes of each specified biometric parameter of every user out of the variety of users, with the identification device being made in accordance with item 32.

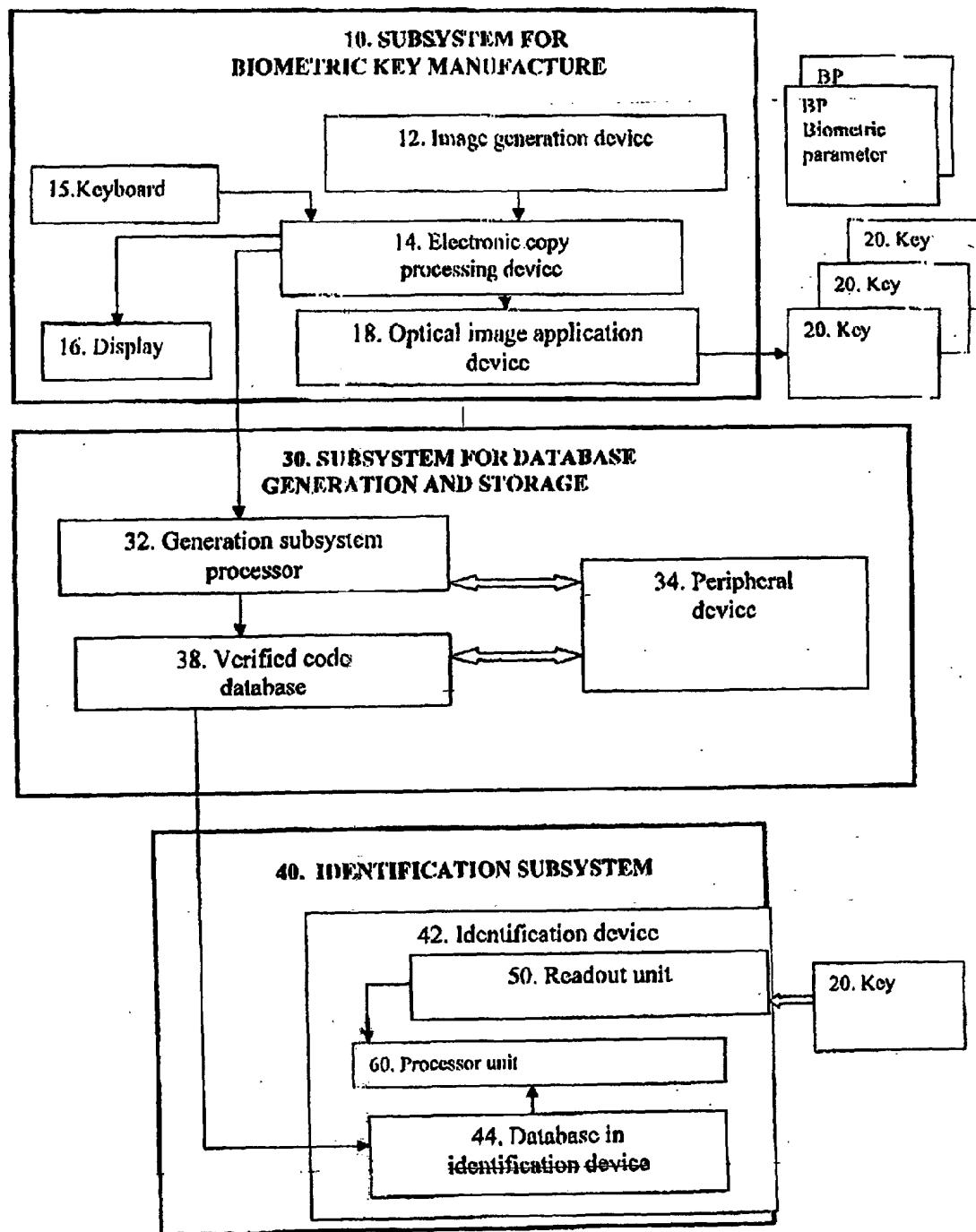


FIG. 1

## 42 Identification device

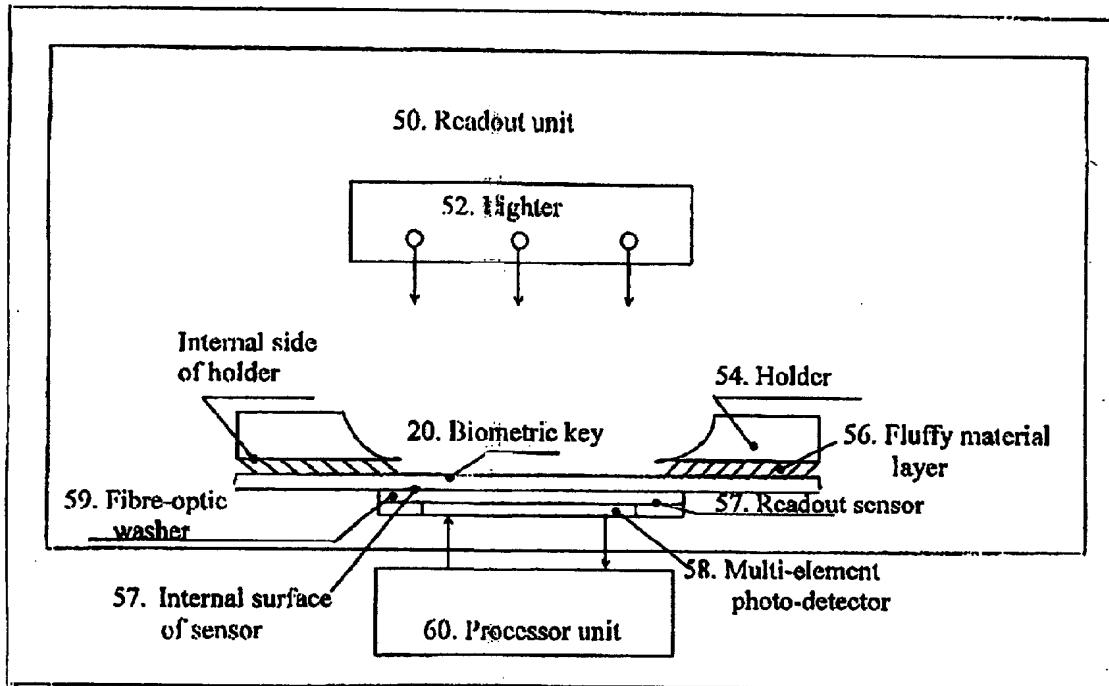


Fig. 3a

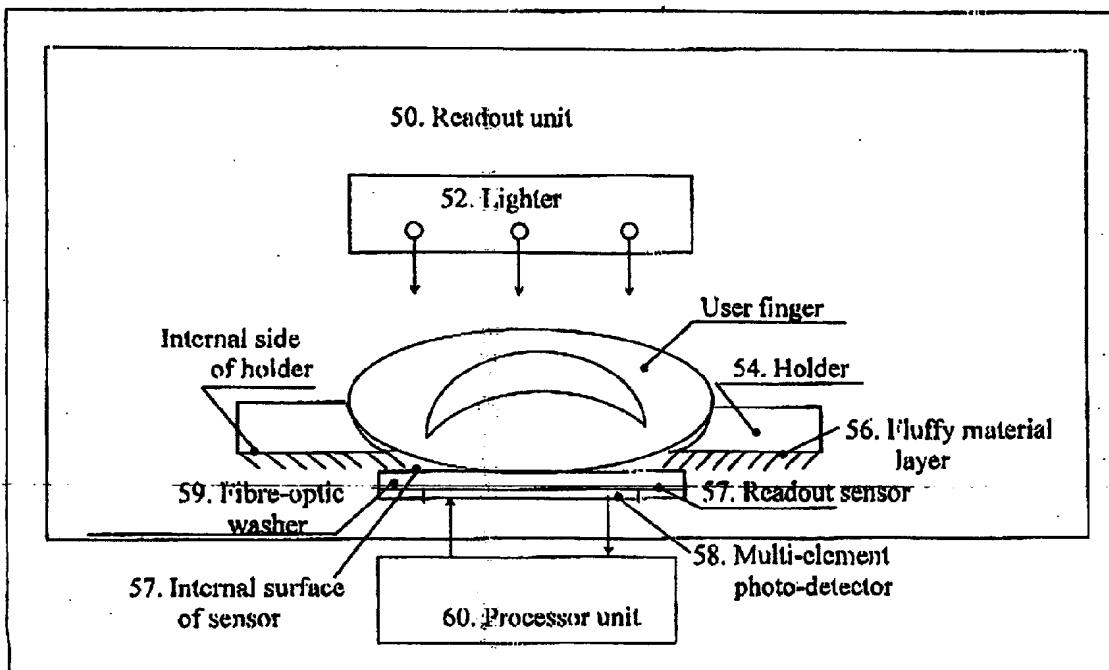


Fig. 3b

## STAGE OF BIOMETRIC KEY MANUFACTURE

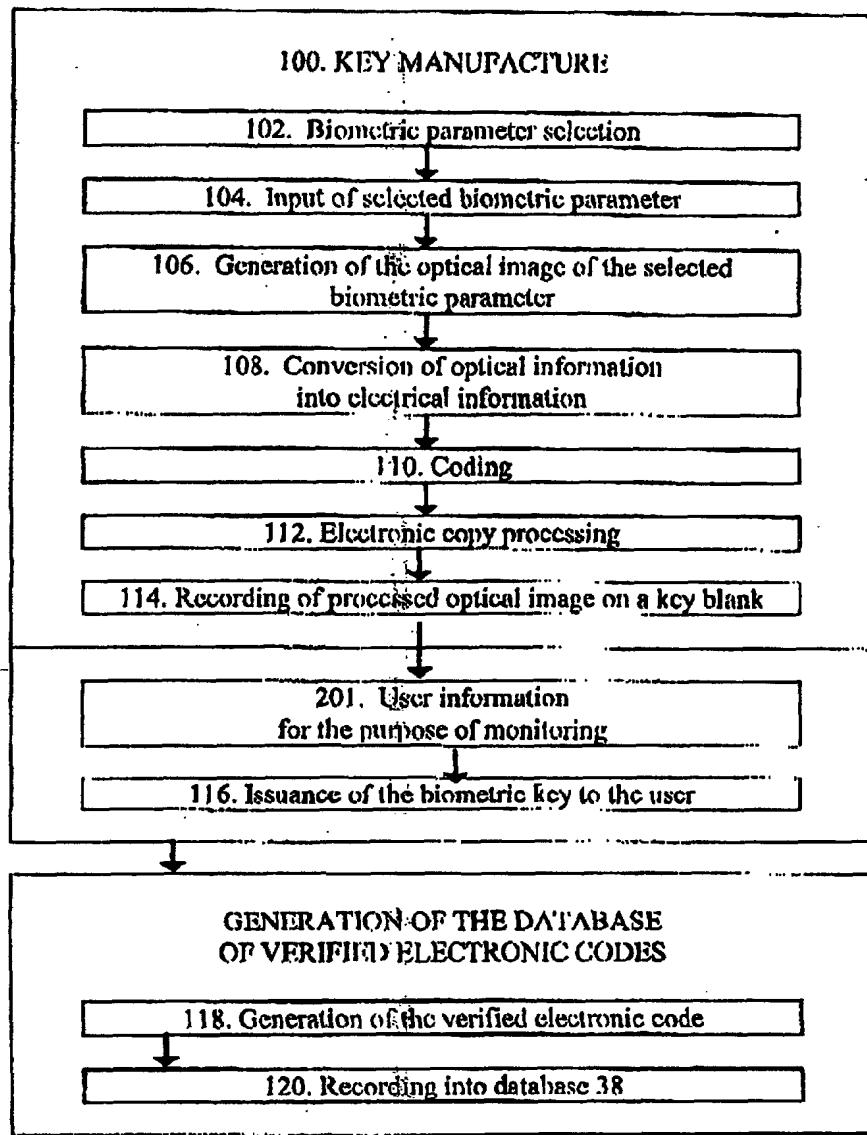


FIG. 4

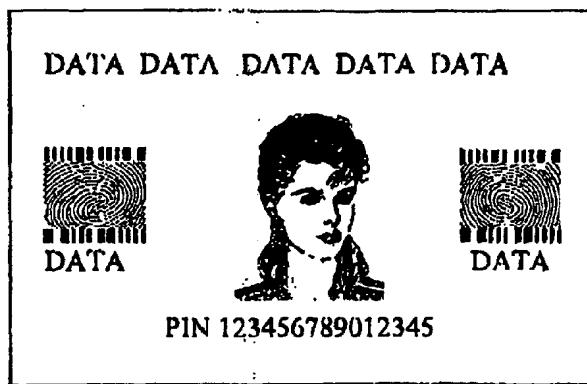


Fig. 2

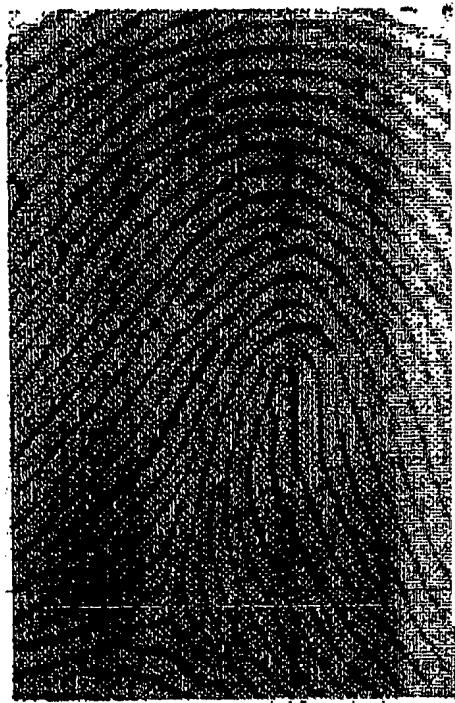


Fig. 5A



Fig. 5B

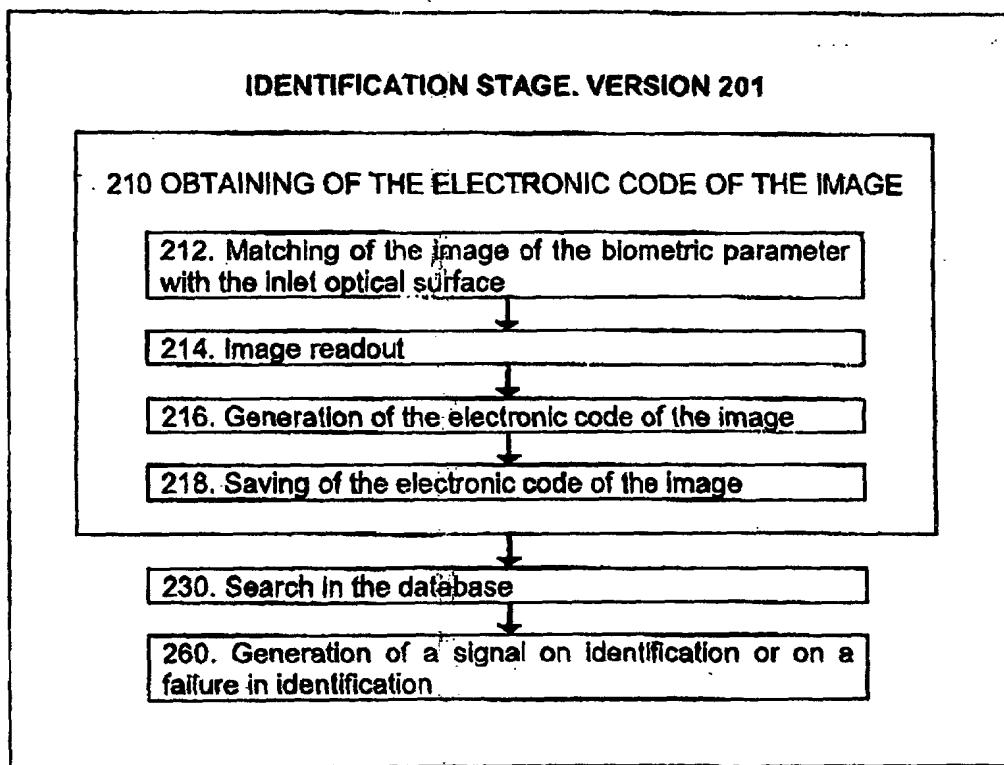


Fig. 6

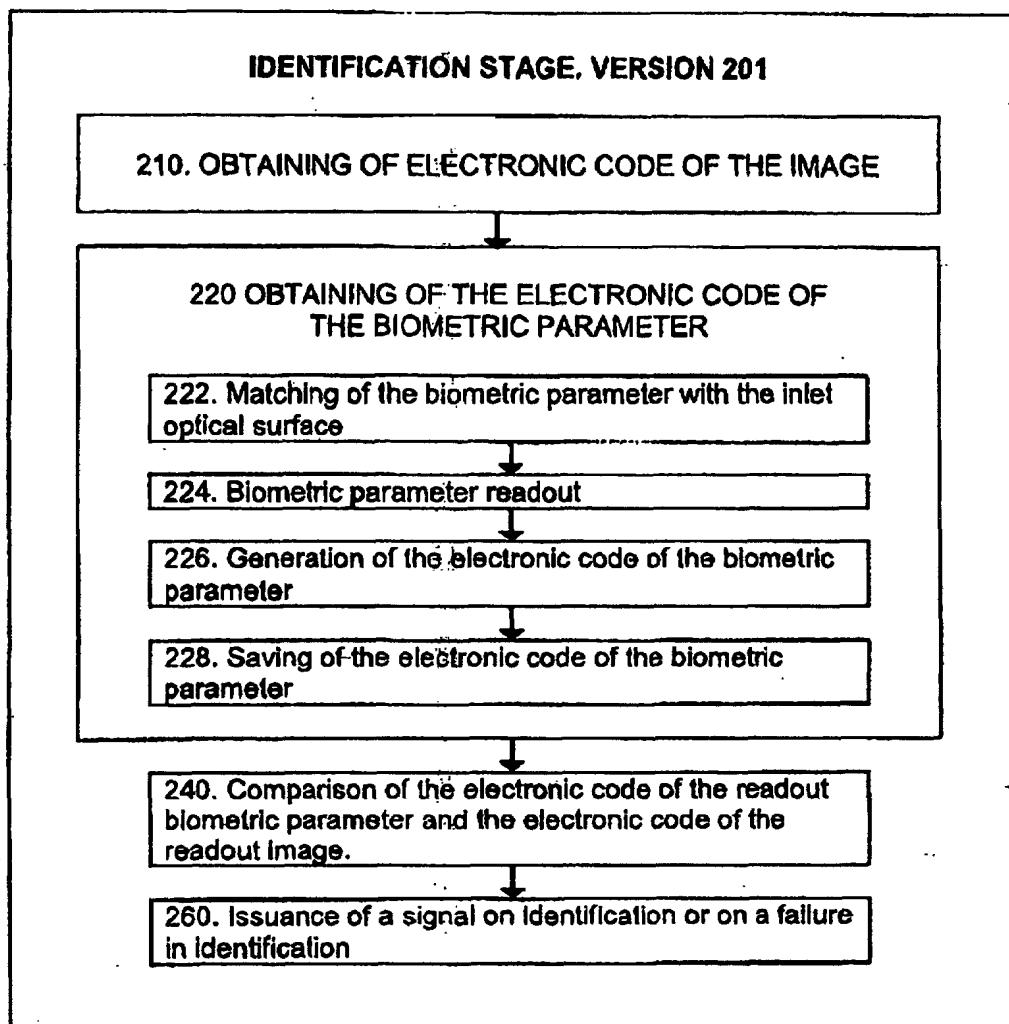


Fig. 7

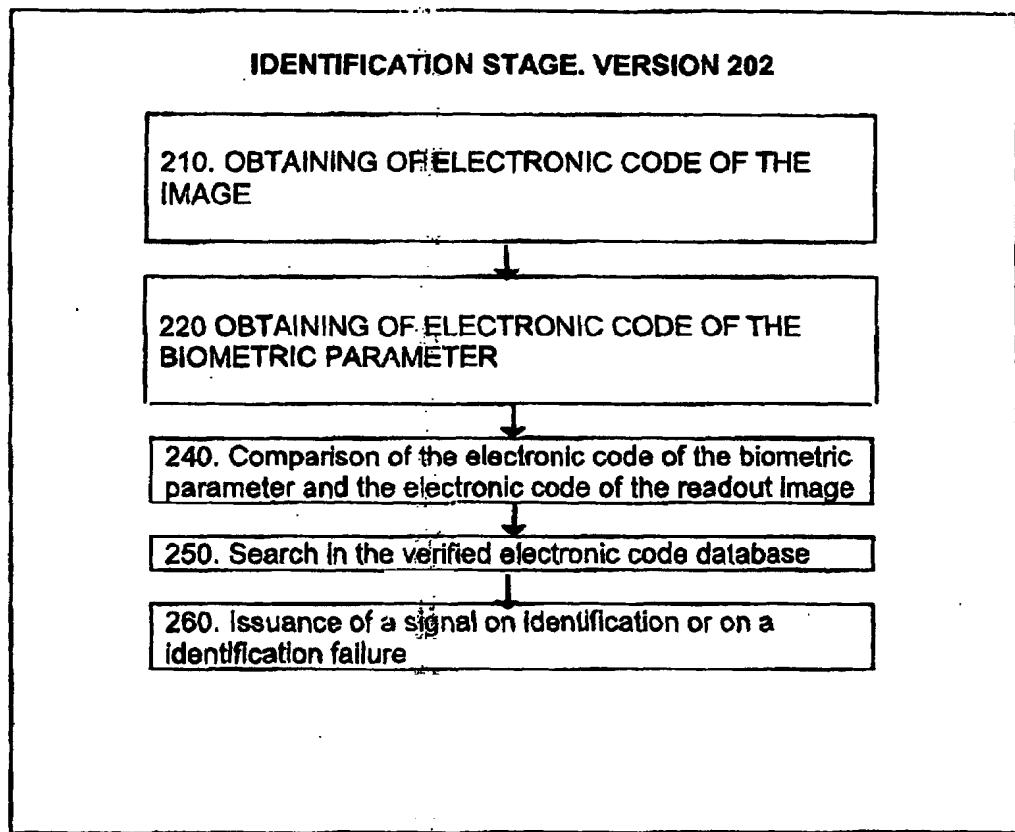


Fig. 8

<b>INTERNATIONAL SEARCH REPORT</b>		International application No PCT/RU																		
<b>A. CLASSIFICATION OF SUBJECT MATTER:</b> IPC 7 G06K 5/00, 19/00, G07F 7/10																				
According to International Patent Classification (IPC) or to both national classification and IPC																				
<b>B. FIELDS SEARCHED</b>  Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06K 5/00, 19/00, G07F 7/10, G07C 9/00, G06K 9/78, 9/00																				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched																				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)																				
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Category</th> <th style="text-align: left; padding: 2px;">Citation of document, with indication, where appropriate, of the relevant passages</th> <th style="text-align: left; padding: 2px;">Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; padding: 2px;">X</td> <td style="padding: 2px;">WO 97/05578 A1 (MYTEC TECHNOLOGIES INC.) 13 February 1997 (13.02.97)</td> <td style="text-align: center; padding: 2px;">1 - 2</td> </tr> <tr> <td style="text-align: center; padding: 2px;">Y</td> <td style="padding: 2px;"></td> <td style="text-align: center; padding: 2px;">3 - 6</td> </tr> <tr> <td style="text-align: center; padding: 2px;">X</td> <td style="padding: 2px;">US 5144680 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 01 September 1992 (01.09.92)</td> <td style="text-align: center; padding: 2px;">17</td> </tr> <tr> <td style="text-align: center; padding: 2px;">X</td> <td style="padding: 2px;">WO 99/66448 A1 (IMAGEWARE SOFTWARE, INC.) 23 December 1999 (23.12.99)</td> <td style="text-align: center; padding: 2px;">1, 10, 17, 21, 23, 33 - 35</td> </tr> <tr> <td style="text-align: center; padding: 2px;">Y</td> <td style="padding: 2px;"></td> <td style="text-align: center; padding: 2px;">4 - 7, 13</td> </tr> </tbody> </table>			Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	WO 97/05578 A1 (MYTEC TECHNOLOGIES INC.) 13 February 1997 (13.02.97)	1 - 2	Y		3 - 6	X	US 5144680 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 01 September 1992 (01.09.92)	17	X	WO 99/66448 A1 (IMAGEWARE SOFTWARE, INC.) 23 December 1999 (23.12.99)	1, 10, 17, 21, 23, 33 - 35	Y		4 - 7, 13
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																		
X	WO 97/05578 A1 (MYTEC TECHNOLOGIES INC.) 13 February 1997 (13.02.97)	1 - 2																		
Y		3 - 6																		
X	US 5144680 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 01 September 1992 (01.09.92)	17																		
X	WO 99/66448 A1 (IMAGEWARE SOFTWARE, INC.) 23 December 1999 (23.12.99)	1, 10, 17, 21, 23, 33 - 35																		
Y		4 - 7, 13																		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C		<input type="checkbox"/> See patent family annex.																		
<ul style="list-style-type: none"> <li>* Special categories of cited documents:</li> <li>"A" document defining the general state of the art which is not considered to be of particular relevance</li> <li>"E" earlier document but published on or after the international filing date</li> <li>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</li> <li>"O" document referring to an oral disclosure, use, exhibition or other means</li> <li>"P" document published prior to the international filing date but later than the priority date claimed</li> </ul> <ul style="list-style-type: none"> <li>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</li> <li>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</li> <li>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</li> <li>"&amp;" document member of the same patent family</li> </ul>																				
Date of the actual completion of the international search report 02 March 2001 (21.03.01)		Date of mailing of the international search report 05 April 2001 (05.04.01)																		
Name and mailing address of the ISA/RU		Authorized officer																		
Facsimile No.		Telephone No.																		

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/RU 00/00446

C. (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4338025 A (ELTON D. ENGEL) Jul. 6, 1982	3-7, 13
A	US 5869822 A (DEXTER L. MEADOWS) Feb. 9, 1999	I-35